CLAIM AMENDMENTS

1. (currently amended) Apparatus for integrating a seller's Web site with a public key infrastructure, wherein:

the public key infrastructure comprises a buyer computer having a Web browser adapted to invoke a signing interface to digitally sign electronic messages and a seller's bank computer system adapted to receive service requests from the seller and to respond to those requests; and

the seller's Web site comprises computer program instructions encoded on at least one computer-readable medium comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

coupled to the filter, an Internet server application adapted to receive redirected HTTP requests from the filter and to process the redirected HTTP requests; and

coupled to the Internet server application, a filter engine adapted to receive processed HTTP requests from the Internet server application and to identify which HTTP requests that contain data requiring require a digital signature by the buyer computer and which requests do not require a digital signature by the buyer computer.

2. (currently amended) The apparatus of claim 1, wherein:

the filter engine is further adapted to identify HTTP requests that require accessing a service offered by the seller's bank and to formulate [[a]] requests for the service; and

the seller's Web site further comprises, coupled to the filter engine, a bank interface adapted to receive requests from the filter engine, reformat the requests, and transmit the requests to the seller's bank.

3. (previously presented) The apparatus of claim 2, wherein the bank interface is further adapted to receive service responses to the requests from the seller's bank, and forward the responses to the filter engine.

4. (previously presented) The apparatus of claim 2, wherein at least one service is certificate validation of a buyer digital certificate.

5. (previously presented) The apparatus of claim 1, wherein the seller's Web site further comprises, coupled to the filter, a Web server adapted to parse requests redirected by the filter.

6. (previously presented) The apparatus of claim 1, wherein services provided by the seller's bank are provided within the context of a four-corner model.

7. (previously presented) The apparatus of claim 6, wherein the four-corner model comprises the buyer, the seller, the seller's bank, and a buyer's bank.

8. (previously presented) The apparatus of claim 1, wherein the filter is implemented using ISAPI.

9. (previously presented) The apparatus of claim 1, wherein the Internet server application is adapted to generate HTTP responses based on data received from the filter engine.

10. (previously presented) The apparatus of claim 1, wherein the Internet server application is adapted to pass hash tables to the filter engine.

11. (previously presented) The apparatus of claim 10, wherein each hash table comprises headers from a redirected HTTP request.

12. (previously presented) The apparatus of claim 10, wherein each hash table indicates a method of the redirected HTTP request.

13. (previously presented) The apparatus of claim 10, wherein each hash table comprises a content-type of a redirected HTTP request.

14. (previously presented) The apparatus of claim 10, wherein each hash table comprises a buyer computer's IP address.

15. (previously presented) The apparatus of claim 10, wherein each hash table comprises actual data in a redirected HTTP request.

16. (previously presented) The apparatus of claim 10, wherein each hash table comprises a unique session ID.

17. (currently amended) A system for integrating a seller's Web site with a public key infrastructure, the Web site comprising a Web server and a Web application, the public key infrastructure comprising a buyer computer comprising a Web browser adapted to invoke a signing interface to digitally sign electronic messages, the public key infrastructure further comprising a seller's bank computer system adapted to receive service requests from the seller and to respond to those requests with digitally signed service responses; the system comprising computer program instructions encoded on at least one computer-readable medium comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

an Internet server application adapted to receive [[a]] redirected HTTP requests from the filter and to process the redirected HTTP requests; and

a filter engine adapted to receive [[the]] processed HTTP requests and to identify [[an]]

-4-

HTTP requests that ~~contains~~ contain data requiring signature by the buyer; wherein:

the Internet server application is a servlet.

18. (previously presented) The system of claim 17, wherein the servlet is constructed as a public class object that extends javax.servlet.http.HttpServlet.

19. (previously presented) The system of claim 18, wherein the public class object comprises at least one of a callFilterEngine method, a doGet method, a doPost method, a getRequestHeaders method, a handle Request method, an init method, a print ErrorResponse method, a printPluginPage method, a readMessage method, a read RequestData method, and a setServletHeaders method.

20. (previously presented) The system of claim 17, wherein the filter engine is adapted to return an object to the servlet.

21. (previously presented) The apparatus of claim 20, wherein the object comprises an integer value indicating one of the following four conditions:

a signature is required on data in the HTTP request;

a response has been received from the seller's bank concerning a service request;

the HTTP request has been passed through to a Web application;

an error occurred.

22. (currently amended) The apparatus of claim 21, wherein when the integer value indicates that a signature is required on data in the HTTP request, the Internet server application stores a state of the filter engine in a cookie and causes a Web page containing the cookie and an instruction to sign [[the]] data to be transmitted to the Web browser.

23. (previously presented) The apparatus of claim 1, wherein the filter engine determines whether an HTTP request contains data requiring signature by applying filtering rules.

24. (previously presented) The apparatus of claim 1, wherein the filter engine is programmed to recognize each HTTP request that includes data requiring a digital signature by the buyer's computer.

25. (previously presented) The apparatus of claim 1, wherein the filter engine is programmed to recognize HTTP requests transmitted by the Web browser that have been modified to include a special tag that indicates whether the request includes data that requires a digital signature by the buyer's computer.

26. (currently amended) A system for integrating a seller's Web site with a public key infrastructure, the Web site comprising a Web server and a Web application, the public key infrastructure comprising a buyer computer comprising a Web browser adapted to invoke a signing interface to digitally sign electronic messages, the public key infrastructure further comprising a seller's bank computer system adapted to receive service requests from the seller and to respond to those requests with digitally signed service responses; the system comprising computer program instructions encoded on at least one computer-readable medium comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

an Internet server application adapted to receive [[a]] redirected HTTP requests from the filter and to process the redirected HTTP requests; and

a filter engine adapted to receive [[the]] processed HTTP requests and to identify [[an]] HTTP requests that contains contain data requiring signature by the buyer; wherein:

the filter engine is implemented as a public class object that extends java.lang.object.

-6-

27. (previously presented) The system of claim 26, wherein the public class object comprises at least one of the following methods: a callWebApp method, a getSessionID method, a newRequestHandler method, an oldRequestHandler method, a service method, and a signedRequestHandler method.

28. (previously presented) The apparatus of claim 1, wherein the filter engine provides an abstracted front end interface via an object oriented computer programming language remote method invocation.

29. (previously presented) The apparatus of claim 1, wherein the filter engine employs a rules class.

30. (currently amended) A system for integrating a seller's Web site with a public key infrastructure, the Web site comprising a Web server and a Web application, the public key infrastructure comprising a buyer computer comprising a Web browser adapted to invoke a signing interface to digitally sign electronic messages, the public key infrastructure further comprising a seller's bank computer system adapted to receive service requests from the seller and to respond to those requests with digitally signed service responses; the system comprising computer program instructions encoded on at least one computer-readable medium comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

an Internet server application adapted to receive [[a]] redirected HTTP requests from the filter and to process the redirected HTTP requests; and

a filter engine adapted to receive [[the]] processed HTTP requests and to identify [[an]] HTTP requests that contains contain data requiring signature by the buyer; and

a rules class, wherein the rules class comprises <u>at least one of</u> the following methods: a getMode method, a getService method, a readRules method, a rulesMatch method, and a validateRules method.

31. (previously presented) The apparatus of claim 1 wherein the seller's Web site further comprises, coupled to the filer engine, a bank interface designed with a plug-in based architecture.

32. (previously presented) The apparatus of claim 1 wherein the seller's Web site further comprises, coupled to the filer engine, a bank interface supporting an abstract front-end interface to allow communication via a plurality of middleware technologies.

33. (previously presented) The apparatus of claim 1 wherein the seller's Web site further comprises, coupled to the filter engine, a bank interface adapted to create and transmit OCSP requests.

34. (previously presented) The apparatus of claim 1 wherein the seller's Web site further comprises, coupled to the filter engine, a bank interface comprising a certificate status check module.

35. (currently amended) A system for integrating a seller's Web site with a public key infrastructure, the Web site comprising a Web server and a Web application, the public key infrastructure comprising a buyer computer comprising a Web browser adapted to invoke a signing interface to digitally sign electronic messages, the public key infrastructure further comprising a seller's bank computer system adapted to receive service requests from the seller and <u>to</u> respond to those requests with digitally signed service responses; the system comprising

computer program instructions encoded on at least one computer-readable medium comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

an Internet server application adapted to receive [[a]] redirected HTTP requests from the filter and to process the redirected HTTP requests; and

a filter engine adapted to receive [[the]] processed HTTP requests and to identify [[an]] HTTP requests that contains contain data requiring signature by the buyer; and

a bank interface, wherein the bank interface comprises a public class object that extends java.lang.object.

36. (currently amended) A system for integrating a seller's Web site with a public key infrastructure, the Web site comprising a Web server and a Web application, the public key infrastructure comprising a buyer computer comprising a Web browser adapted to invoke a signing interface to digitally sign electronic messages, the public key infrastructure further comprising a seller's bank computer system adapted to receive service requests from the seller and to respond to those requests with digitally signed service responses; the system comprising computer program instructions encoded on at least one computer-readable medium comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

an Internet server application adapted to receive [[a]] redirected HTTP requests from the filter and to process the redirected HTTP requests; and

a filter engine adapted to receive [[the]] processed HTTP requests and to identify [[an]] HTTP requests that contains contain data requiring signature by the buyer; and

a public class object, wherein the public class object comprises at least one of a createOCSPRequest method, a getCertificateID method, a getCertStatus method, a getCertsVerifyMessage method, a getURL method, an isResponseSuccessful method, a

logAndBuildReturnObject method, a processOCSP method, a sendAndReceiveMessage method, a serviceRequest method, and a verifyResponseSignature method.

37. (currently amended) Apparatus for integrating a seller's Web site with a public key infrastructure, said apparatus comprising:

a Web server located at the seller's Web site;

a Web application coupled to the Web server and also located at the seller's Web site, the Web application adapted to:

identify [[those]] which HTTP requests from a buyer that include data requiring require a digital signature of the buyer and which HTTP requests do not require a digital signature of the buyer;

for each HTTP request requiring a digital signature, create a Web page for transmission to a browser controlled by the buyer, said Web page causing the browser to invoke a signing interface enabling the buyer to digitally sign the data, said signing interface comprising a smart card containing a private key associated with the buyer; and

identify [[those]] which HTTP requests [[that]] require a service provided by an entity other than the seller and which HTTP requests do not require a service provided by an entity other than the seller; and

coupled to the Web application and also located at the seller's Web site, an interface module adapted to receive from the Web application requests for service from the Web application entities other than the seller, to format and transmit the requests, to receive responses to the requests, and to forward the responses to the Web application.